UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Plaintiff,

v.

Bradley A. Stetkiw,

Defendant.

Case No. 18-20579
Honorable Victoria A. Roberts

ORDER DENYING STETKIW'S MOTION TO SUPPRESS EVIDENCE OBTAINED OUTSIDE THE SCOPE OF THE SEARCH WARRANT [ECF No. 20]

Before the Court is Defendant Bradley Stetkiw's ("Stetkiw") Motion to Suppress Evidence Obtained Outside the Scope of the Search Warrant. For the reasons explained, the Court **DENIES** the motion.

BACKGROUND

Homeland Security Investigations ("HSI") initially focused an investigation on Stetkiw's Bitcoin exchange service. The Government obtained a search warrant which authorized a computer search for image and data files. While searching Stetkiw's computer, HSI Special Agent William Osborn discovered one image of child pornography. He immediately stopped the computer search and obtained a search warrant

for child pornography. With that warrant, the Government discovered additional images of child pornography.

The Government charged Stetkiw with violations of: 18 U.S.C. § 2252A for receipt and possession of child pornography; 18 U.S.C. §§ 1960 and 2 for operating an unlicensed Bitcoin exchange service; and 18 U.S.C. §§ 2253 and 982 for criminal forfeiture.

Stetkiw filed a Motion to Suppress Evidence Obtained Outside the Scope of the Search Warrant and requested an evidentiary hearing.

MOTION TO SUPPRESS EVIDENCE AND RESPONSE

Stetkiw seeks to suppress child pornography evidence derived from the computer search. He argues that Agent Osborn's computer search for image files was unreasonable and violated the Fourth Amendment. He says the *Leon* good-faith exception is inapplicable because Agent Osborn failed to use techniques like Optimal Character Recognition ("OCR") to narrow the search. OCR scans images for letters or numbers; if used, Stetkiw argues the examiner could have narrowed the search to only images with specific letters or numbers. OCR is not protocol for HSI investigations.

The Government argues that the search warrant and accompanying affidavit established probable cause to search image files. The Government says the plain view doctrine and the *Leon* good-faith exception require the Court to deny suppression.

ANALYSIS

I. THE FOURTH AMENDMENT AND COMPUTER SEARCHES

The Fourth Amendment of the Constitution states ". . . no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. A search or seizure must satisfy traditional reasonableness standards by balancing an individual's privacy interests against legitimate governmental interests. *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999).

In 2014, the Supreme Court required officers to secure search warrants for cell phones because "they hold for many Americans 'the privacy of life.'" *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Unlike home searches, searches of electronic devices offer less predictable, specific, and discrete

regions to search. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 538 (2005).

The Sixth Circuit held that "a computer search may be as extensive as reasonably required to locate items described in the warrant based on probable cause." *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011) (citing *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir. 2009)). Indeed, the Court held that if "the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officer to open various types of files located in the computer's hard drive to determine whether they contain such evidence." *Id.* at 540.

A search warrant for computers satisfies the Fourth Amendment particularity requirement if it is limited to a specific federal crime or specific material. *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005). *See, e.g.*, *United States v. Ulbricht*, 858 F.3d 71, 101 (2d Cir. 2017), *cert. denied* 138 S.Ct. 2708 (2018); *United States v. Wong*, 334 F.3d 831, 837-38 (9th Cir. 2003).

II. THE SEARCH WARRANT WAS PARTICULAR

Attachment B to the search warrant authorized agents to seize evidence related to Stetkiw's alleged violation of 18 U.S.C. § 1960. The

search warrant authorized a seizure of "stored records or information that is otherwise called for by this warrant" (ECF No. 20-2, PageID.78). The warrant defines "records" and "information" as "all forms of creation or storage, including . . . photographic form" (ECF No. 20-2, PageID.80). During the evidentiary hearing, HSI Special Agent Bryan Randall testified that searching image and data files was necessary because Stetkiw could store Bitcoin evidence anywhere on the computer.

For these reasons, the Court finds the warrant was sufficiently particular concerning the evidence to be seized and locations to be searched.

III. PROBABLE CAUSE EXISTED TO SEARCH IMAGE FILES

The Sixth Circuit explained that probable cause for a search warrant "exists when there is a 'fair probability,' given the totality of circumstances, that contraband or evidence of a crime will be found in a particular place." *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir. 1991) (quoting *United States v. Loggins*, 777 F.2d 336, 338 (6th Cir. 1985)). To establish probable cause, the Court "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." *United States v.*

McClain, 444 F.3d 556, 562-63 (6th Cir. 2005) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)).

Stetkiw argues that the warrant did not authorize a search of his image files. He says, "no reasonable officer should be looking at image files when looking for Bitcoin transactions" (ECF No. 20, PageID.44). The Court disagrees.

The search warrant established that relevant substantive evidence could be found in image files; Bitcoin owners "hide [private keys and wallet addresses] in various places . . ." (ECF No. 28-2, PageID.229). Additionally, during the evidentiary hearing Agent Randall testified that Agent Osborn searched Stetkiw's image files for: (1) Quick Response ("QR") codes, barcodes used to store information on a smartphone; (2) seed keys, a string of words used to recover a Bitcoin wallet; and (3) Bitcoin wallet passwords. He explained Bitcoin owners can take photos of deposit receipts to confirm transactions and sometimes take selfies with their Bitcoin passwords to confirm identity.

The affidavit also established that image files contain attribution evidence: evidence of who used, owned, or controlled the device; the computer user's physical location; and state of mind. *See United States v.*

Gholston, 993 F.Supp.2d 704, 708 n.2 (E.D. Mich. 2014) ("'user attribution' evidence typically found on a cell phone, which 'indicate[s] who has used or controlled the device,' is analogous to the 'indicia of occupancy' that officers look for 'while executing a search warrant at a residence.'").

Although Stetkiw's expert, William Green, testified that it is uncommon to find Bitcoin evidence in image files, he conceded that it was possible to find both substantive and attribution evidence in image files.

The affidavit and testimony during the evidentiary hearing established that relevant substantive and attribution could be found in image files. The Court finds that probable cause existed to search Stetkiw's image files.

IV. SEARCHING IMAGE FILES WAS REASONABLE

Reasonableness for computer searches is fact specific and is applied on a case-by-case basis. *Richards*, 659 F.3d at 539. The Supreme Court said "[i]t is generally left to the discretion of the executing officers to determine the detail of how best to proceed with the performance of a search authorized by warrant . . . ." *Dalia v. United States*, 441 U.S. 238, 257 (1979). *But see United States v. Comprehensive Drug Testing*, 579 F.3d 998, 1006 (9th Cir. 2009).

Stetkiw argues searching image files was unreasonable because the agent failed to use OCR. While the Court recognizes Stetkiw's heightened privacy concerns in the computer context, the Court disagrees and finds that the search was reasonable.

Because individuals can "hide, mislabel, or manipulate files to conceal criminal activity, a broad expansive search of the hard drive may be required." *United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011); *see also Burgess*, 576 F.3d at 1092-94; *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010); *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006).

HSI Special Agent David Alley testified that individuals can disguise image files. A "pinpointed computer search . . ." may prevent agents from discovering images saved under disguised names. *Adjani*, 452 F.3d at 1150-51. "The [G]overnment should not be required to trust the suspect's self-labeling when executing a warrant." *Id.* at 1150.

Regardless of whether the agent used OCR, Agent Osborn acted reasonably when he searched image files related to Stetkiw's alleged violation of 18 U.S.C. § 1960.

V. CHILD PORNOGRAPHY WAS IN PLAIN VIEW

The plain view doctrine allows evidence obtained without a warrant to come in when: (1) the officer was lawfully in a position from which to view the object seized in plain view; (2) the object's incriminating character was immediately apparent—i.e., the officer had probable cause to believe the object was contraband or evidence of a crime; and (3) the officer had a lawful right of access to the object itself. *United States v. Soussi*, 29 F.3d 565, 570 (10th Cir.1994) (citing *Horton v. California*, 496 U.S. 128, 134 (1990)).

The Government argues that the image of child pornography was in plain view. Stetkiw refers to *United States v. Carey* which held that images of child pornography "were in closed files and thus not in plain view." *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999). However, *Carey's* holding was limited to the "subsequent opening of numerous files the officer knew, or at least expected, would contain images of child pornography;" it did not apply to the first discovered image of child pornography. *Id.* at 1273 n.4. *Carey* is distinguishable from this case because Agent Osborn stopped searching the computer after he discovered one image of child pornography.

The Sixth Circuit found that if the search warrant established probable cause to search an area of a computer, officers may search that area to determine whether it contains relevant evidence. *See Richards*, 659 F.3d at 558. Here, the warrant established probable cause to search Stetkiw's image files for Bitcoin evidence. When Agent Osborn discovered one image of child pornography, that image in that file was in plain view.

The Court finds that in this specific case, the plain view doctrine provides ground to admit the first image of child pornography discovered. All subsequent images were discovered pursuant to a lawfully issued second search warrant and are admissible.

VI. AGENT OSBORN ACTED IN GOOD-FAITH

Assuming the search of Stetkiw's image files was unlawful and unreasonable, the *Leon* good-faith exception would not cause the Court to suppress the evidence. The *Leon* good-faith exception "allows admission of evidence 'seized in reasonable, good-faith reliance on a search warrant that is . . . defective.'" *United States v. Leon*, 468 U.S. 897, 905 (1984).

When officers inadvertently discovered child pornography during a computer search for a different crime, the officer must cease the search and obtain a separate warrant for child pornography. *See United States v.*

Lucas, 640 F.3d 168, 179 (6th Cir. 2011); *United States v. Walser*, 275 F.3d 981, 985 (10th Cir. 2001). This is precisely what Agent Osborn did: when he discovered child pornography he stopped the search, contacted Agent Randall, and obtained a separate warrant for child pornography.

Under the Fourth Amendment, the warrant was particular and supported by probable cause; it was not facially deficient in describing the items to be seized and searched. *Richards*, 659 F.3d at 542. For these reasons, there is no indication that agents deliberately strayed from the search warrant; the *Leon* good-faith exception would only apply if the warrant was defective.

VII. RECOMMENDATION FOR *EX ANTE* REVIEW OF SEARCH PROCEDURES

While the search in this case was constitutionally conducted, testimony given by Agent Randall during the evidentiary hearing is concerning.

He testified that there were no practical limitations to what could be searched for on Stetkiw's computer. The warrant to investigate Stetkiw's Bitcoin exchange service does not explicitly reflect that sentiment; that may have prevented the magistrate judge from contemplating it or asking any questions concerning limitations.

To address this issue, the Court recommends adopting more rigorous *ex ante* review of warrants to search electronically stored information ("ESI").

An *ex ante* review is the magistrate judges' review of all warrant applications as required by the Supreme Court; approval of a warrant request is dependent on a showing of probable cause as described in the Constitution. *See Dalia* 441 U.S. at 255-56. The permissible breadth of a warrant is linked to showing probable cause that demonstrates "the evidence sought will aid in the particular apprehension or conviction" for an offense. *Id.* at 255. By contrast, a court conducts *ex post* review when it examines the constitutionality of a search after its execution. The Court's opinion in this case is an *ex post* review.

Currently, in this district, magistrate judges' *ex ante* reviews of applications to search ESI generally permit the search of an entire device to find responsive materials without reviewing the Government's intended protocols for the search. This can be problematic.

Given the wealth of ESI stored on a computer there is greater risk a warrant to search someone's personal device will turn into a general warrant. *Comprehensive Drug Testing*, 621 F.3d at 1176; *see also Richards*, 659 F.3d at 537. However, despite this risk, *ex post* courts do not

require ESI search protocols. *See Richards*, 659 F.3d at 538-39 (declining to impose mandatory protocols to satisfy particularity); *see also Ulbricht*, 858 F.3d at 102 (finding that specific protocols are not required to prevent a search warrant from becoming overbroad for lack of particularity).

These judicial reservations are based on a fear of telling investigators how to conduct investigations and what could result from such limitations; there is concern that individuals might hide information in a way that forces a protocol-bound investigator to overlook it, as discussed before. *See Ulbricht*, 858 F.3d at 102.

The Court finds that an *ex ante* "minimization" requirement can address concerns about potential Fourth Amendment violations of protocol-less searches, with a goal of decreasing the amount of non-responsive ESI encountered in a search. *See* Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 EMORY L.J. 49, 55 (2018) (discussing the relationship between *ex ante* review of search protocols and minimization requirements for other warrants that permit the search of broadly seized information like wiretaps). Developing that requirement can also address concerns about how protocols might render searches ineffective.

A process to review ESI search protocols *ex ante* does not mean that search protocols would be mandated in all cases; protocols would be approved on a case-by-case basis.

E*x ante* review of the Government's procedures to search ESI has advantages. First, it can minimize the need for *ex post* review of those procedures, which is often contentious as parties debate motions to suppress evidence in criminal cases. Second, it allows a magistrate judge to closely work with the Government to ensure its preferred procedures do not violate the Fourth Amendment. Third, it can promote the development of case law that can distinguish permissible and impermissible procedures to better protect Fourth Amendment rights. Finally, it could prevent situations where certain file locations are authorized for search by warrant, but the practical implications of that authorization create a general warrant without the magistrate judge's knowledge.

Ex ante review is a flexible system where the magistrate judge can balance the needs of an investigation and the demands of the Fourth Amendment. Certain procedures may be found inappropriate in certain contexts depending on the extent of probable cause the Government has, but that is distinct from mandating that the Government follow a specific procedure. *Ex ante* review is flexible enough that the Government can opt

to apply for a warrant with no procedures or minimization and still be approved.

However, in such cases the Government should demonstrate that the level of probable cause to search ESI is high enough to justify a search without minimization. Additionally, even if a no-protocol approach is appropriate at the outset, it is recommended the Government return to the reviewing judge to confirm that searching the ESI without a protocol is appropriate after the investigation proceeds far enough for that information to become available.

The Court recommends that the Government submit the procedural steps it will take to minimize searching non-responsive ESI in its warrant applications. It is also recommended that magistrate judges deny applications if they find the Government has not proposed sufficient means to minimize the search of non-responsive ESI, given the extent of probable cause shown. If the Government needs to change its procedures mid-investigation, it is encouraged to return to the magistrate judge for approval.

CONCLUSION

The search of Stetkiw's computer files and seizure of child pornography images was constitutionally permissible. However, Stetkiw

raises legitimate privacy issues that are worthy of debate. For that reason, the Court recommends additional *ex ante* review of future search warrants for ESI, with a goal to balance individual privacy interests against legitimate governmental interests.

The Court **DENIES** Stetkiw's Motion to Suppress Evidence Obtained Outside the Scope of the Search Warrant.

IT IS ORDERED.

s/ Victoria A. Roberts
Victoria A. Roberts
United States District Judge

Date: 7/3/2019